Daily Open Source Infrastructure Report
27 August 2015

Top Stories

- Officials announced August 25 that Kraft Heinz Foods Company issued a recall for more than 2 million pounds of its turkey bacon products due to adulteration.– *U.S. Department of Agriculture* (See item **9**)
- Police took a teenager into custody following negotiations after the juvenile held 29 students and a teacher hostage at Philip Barbour High School in West Virginia August 25. – *Fox News; Associated Press* (See item **16**)
- Crews reached 15 percent containment August 25 of the 258,339-acre Okanogan Complex Fire burning in Washington and officials reported that the fire remains the top priority in the U.S.– *NBC News* (See item **23**)
- A reporter and photographer from a local news station in Virginia were killed by a shooter that appeared during a live news interview at Bridgewater Plaza in Moneta, Virginia August 26. – *WTKR 3 Norfolk* (See item **34**)

Fast Jump Menu

Energy Sector

1. *August 25, Reuters* – (New Jersey) **Exxon $225 mln pollution settlement with New Jersey is approved.** A $225 million settlement between ExxonMobil Corp and the State of New Jersey was approved August 25 following allegations that Exxon damaged over 1,500 acres of wetlands and marshes and contaminated natural resources for decades through its refinery operations in Bayonne and Linden, as well as thousands of other facilities throughout the State. The agreement also ensures the prompt cleanup of hazardous substances.
Source: http://www.reuters.com/article/2015/08/25/exxon-mobil-new-jersey-settlement-idUSL1N1101P220150825

2. *August 25, Associated Press* – (North Dakota) **Ex-well operator in North Dakota indicted in dumping case.** A Southlake, Texas man was indicted August 24 on multiple felony charges related to an illegal wastewater dumping case in which saltwater was injected into the Halek 5-22 disposal well in North Dakota without the approval or witness of State inspectors, following a failed pressure test. The man allegedly worked with a co-conspirator to mislead officials while dumping the wastewater into the disposal well between December 2011 and February 2012.
Source: https://eaglefordtexas.com/news/id/156540/ex-well-operator-in-north-dakota-indicted-in-dumping-case-2/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

3. *August 26, CapeCod.com* – (Massachusetts) **Pilgrim returns to full power after shutdown, repairs.** Entergy officials reported that the Pilgrim Nuclear Power Station in Plymouth was returned to full power August 26 after replacing a broken instrument control line feeding a plant main steam isolation valve that caused an automatic shutdown of the reactor over the weekend of August 22.
Source: http://www.capecod.com/newscenter/pilgrim-returns-to-full-power-after-shutdown-repairs/

4. *August 25, WLS 7 Chicago* – (Illinois) **Federal authorities investigate guns missing from LaSalle nuclear plant.** The U.S. Nuclear Regulatory Commission and local law enforcement were investigating after Exelon officials reported that two 9 millimeter handguns were stolen from the security arsenal at the LaSalle Nuclear Generating Station in Marseilles July 27.
Source: http://abc7chicago.com/news/authorities-investigate-guns-missing-from-lasalle-nuclear-plant/956975/

Critical Manufacturing Sector

5. *August 25, U.S. Consumer Product Safety Commission* – (National) **Osram Sylvania**

recalls T8 LED tubes due to burn hazard. Osram Sylvania Inc., issued a recall for about 46,300 SubstiTUBE IS T8 LED lamps due to an issue which could cause lamps to overheat and melt. The product was distributed at Osram Sylvania industrial and commercial distributors from December 2014 – May 2015.
Source: http://www.cpsc.gov/en/Recalls/2015/Osram-Sylvania-Recalls-T8-LED-Tubes/?utm

6. *August 25, U.S. Department of Labor* – (Georgia) **Atlanta's American Air Filter Co. continues to expose workers to serious safety hazards.** The Occupational Safety and Health Administration cited Atlanta-based American Air Filter Co. Inc., with 5 violations for failing to provide proper machine guarding to protect employees from amputation hazards and for not following procedures to prevent machinery from inadvertently starting up during servicing and maintenance. Proposed penalties total $119,900.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28608

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

7. *August 25, Reuters* – (New York) **Man linked to rejected AmEx accord admits cheating NY law firms.** A man whose wife was tied to a recently rejected antitrust settlement between retailers and American Express Co pleaded guilty August 25 to charges that he and his wife defrauded 2 New York law firms out of $7.8 million through the use of bogus limited liability corporations for litigation support services that he never performed.
Source: http://www.reuters.com/article/2015/08/25/lawfirms-fraud-idUSL1N1102OQ20150825

For another story, see item **15**

Transportation Systems Sector

8. *August 26, Mississippi News Now* – (Mississippi) **U.S. Highway 84 still closed following tanker accident.** All lanes of U.S. 84 at Mississippi State Highway 184 in Lawrence County remained closed August 26 following an accident involving an overturned semi-truck that shutdown lanes August 25. The driver of the semi-truck attributed the crash to failed brakes and escaped with minor injuries.
Source: http://www.myfoxal.com/story/29877222/overturned-tanker-closes-all-lanes-of-us-highway-84

Food and Agriculture Sector

9. *August 26, U.S. Department of Agriculture* – (International) **Kraft Heinz Foods Company recalls turkey bacon products due to possible adulteration.** The Food Safety and Inspection Service announced August 25 that Kraft Heinz Foods Company issued a recall for more than 2 million pounds of its turkey bacon products due to adulteration that could cause the products to spoil prior to the "Best When Used By" date. The products were sold nationwide and exported to the Bahamas and St. Martin.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-113-2015-release

10. *August 25, Food Safety News* – (Michigan) **Michigan officials warn public about products made in unlicensed facility.** The Michigan Department of Agriculture and Rural Development issued a warning to consumers to immediately dispose of all Brandy's "Jam"boree-N-More, Brandy & Dutch Weigand, and Pier III products purchased at various State farmers markets and festivals, due to the products being manufactured in an unlicensed facility lacking quality controls.
Source: http://www.foodsafetynews.com/2015/08/michigan-officials-warn-public-about-products-made-in-unlicensed-facility

11. *August 25, U.S. Food and Drug Administration* – (National) **JO's Candies issues voluntary alert on undeclared milk in Dark Chocolate covered Honey Grahams with Sea Salt.** California-based Jo's Candies issued a voluntary recall August 25 for its Trader Joe's brand Dark Chocolate covered Honey Grahams with Sea Salt products due to mislabeling and undeclared milk. Two reactions were reported by consumers, and the affected products were distributed nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm459770.htm

12. *August 25, KARE 11 Minneapolis* – (Minnesota) **Emerald ash borer infestation found in Scott County.** The Minnesota Department of Agriculture placed Scott County, Minnesota, under an emergency quarantine August 25 after the discovery of an emerald ash borer in a tree on private property. Scott County joined the nine other counties in the State under quarantine.
Source: http://www.kare11.com/story/news/outdoors/2015/08/25/emerald-ash-borer-infestation-found-in-scott-county/32335391/

13. *August 25, Food Safety News* – (National) **CDC: 495 in 30 states now have Cyclospora infection, possibly from cilantro.** The U.S. Centers for Disease Control and Prevention announced August 25 that 495 individuals from 30 States had confirmed cases of Cyclospora infections, linked to imported cilantro. Authorities continue to investigate the outbreak.
Source: http://www.foodsafetynews.com/2015/08/cdc-update-457-people-in-29-states-confirmed-with-cyclospora-infection/#.Vd3T7flVhBe

Water and Wastewater Systems Sector

14. *August 25, Vicksburg Post* – (Mississippi) **City's water treatment facility loses**

power, thousands ordered to boil water. Officials issued a boil water notice for thousands of Vicksburg residents after the Vicksburg Water Treatment facility on Haining Road lost power August 25. Power was restored to the plant and the order is in effect for the entire city until further notice.
Source: http://www.vicksburgpost.com/2015/08/25/citys-water-treatment-facility-loses-power-thousands-ordered-to-boil-water/

Healthcare and Public Health Sector

15. *August 25, U.S. Securities and Exchange Commission* – (Indiana) **SEC obtains summary judgement against Indianapolis resident in securities fraud involving biomedical company.** The U.S. Securities and Exchange Commission announced August 24 a summary judgement against an Indianapolis resident after an investigation determined that he violated the antifraud provisions of the Federal securities laws by misleading the public and making false statements about Xytos, Inc., a company he controlled. Officials alleged that the individual intentionally misled the public and published that the company treated cancer patients while selling shares of the company in unregistered open market transactions.
Source: http://www.sec.gov/litigation/litreleases/2015/lr23328.htm

For another story, see item **19**

Government Facilities Sector

16. *August 26, Fox News; Associated Press* – (West Virginia) **Police say 14-year-old boy held class, teacher hostage at West Virginia school.** Police took a teenager into custody following negotiations after the juvenile held 29 students and a teacher hostage at Philip Barbour High School in Philippi, West Virginia, August 25. The school was placed on a lockdown and other students were moved out of the building while authorities responded to the scene after reports of an individual with a gun.
Source: http://www.foxnews.com/us/2015/08/25/cops-suspect-isolated-students-safe-in-hostage-like-situation-at-school/

17. *August 26, Washington Post* – (Washington, D.C.) **Washington Monument to reopen Wednesday morning; elevator fixed.** The Monument in Washington, D.C., was scheduled to reopen August 26 following repairs, after it was closed August 25 due to a "door contacts" issue with the elevator that caused about 60 people to evacuate down the stairs.
Source: http://www.washingtonpost.com/news/local/wp/2015/08/26/washington-monument-elevator-breaks-again/

18. *August 25, Cincinnati Enquirer* – (Ohio) **Suspicious package scare causes school evacuation.** Students from North Avondale Montessori School in Cincinnati were evacuated and classes were dismissed August 25 after a school resource officer reported a suspicious package on Clinton Springs Avenue. Police investigated and cleared the scene after determining that there was no threat.
Source: http://www.cincinnati.com/story/news/2015/08/25/emergency-officials-

respond--suspicious-package--avondale-school/32324177/

19. *August 25, Champaign-Urbana News-Gazette* – (Illinois) **Number of mumps cases nears 100 in local outbreak; more clinics set.** Health officials in Champaign-Urbana set up additional free, all-day vaccination clinics following 98 confirmed cases of the mumps August 25 that have been linked to the University of Illinois campus. Authorities urged students, staff, and faculty to receive a third dose of the vaccine in hopes of getting the outbreak under control.
Source: http://www.news-gazette.com/news/local/2015-08-25/updated-number-mumps-cases-nears-100-local-outbreak-more-clinics-set.html

20. *August 25, Associated Press* – (California) **Audit: California agencies vulnerable to IT security breach.** A report released August 25 by the State auditor found that several California agencies were not in compliance with the State's information technology standards, leaving them vulnerable to potential attacks and security breaches, among other findings. The California Department of Technology responded that it is committed to improving the State's overall security posture and oversight.
Source: http://www.dailyherald.com/article/20150825/business/308259843/

21. *August 25, KTVB 7 Boise* – (Idaho) **Red Cross helping Clearwater Complex fire victims.** Crews worked August 25 to contain multiple, individual fires that burned together and formed the Clearwater Complex, Municipal Complex, and Motorway Complex fires, which have charred over 47,260 acres in Idaho.
Source: http://www.ktvb.com/story/news/local/idaho/2015/08/26/red-cross-helping-clearwater-complex-fire-victims/32371451/

22. *August 25, KPIX 5 San Francisco; San Francisco Bay City News* – (California) **3rd Lake County fire now fully contained after burning 25,000 acres.** Crews reached full containment August 24 of the Jerusalem Fire that burned over 25,000 acres in Lake and Napa counties. Firefighters continued to battle the Wragg Fire and Rocky Fire that has burned more than 77,000 acres across California.
Source: http://sanfrancisco.cbslocal.com/2015/08/25/3rd-lake-county-fire-now-fully-contained-after-burning-25000-acres/

23. *August 25, NBC News* – (Washington) **Resources falling short as Washington wildfire grows into historic monster.** Crews reached 15 percent containment August 25 of the 258,339-acre Okanogan Complex Fire burning in Washington. Officials reported that the fire remains the top priority in the U.S. and additional resources were being diverted from California.
Source: http://www.nbcnews.com/storyline/western-wildfires/resources-falling-short-washington-wildfire-grows-historic-monster-n415911

Emergency Services Sector

24. *August 25, San Francisco Chronicle* – (California) **Gun, badge stolen from Calif. University police chief's unmarked car.** Authorities are searching for the thieves who stole a loaded gun, ammunition, police badge, and a department-issued laptop August

24 from an unmarked vehicle parked near the Point Isabel Regional Shoreline in Richmond, belonging to the University of California, Berkeley police chief.
Source: http://www.policeone.com/investigations/articles/8720853-Gun-badge-stolen-from-Calif-university-police-chiefs-unmarked-car/

25. *August 25, Chico Enterprise-Record* – (California) **9-1-1 system restored in Butte County.** Emergency 9-1-1 service for Butte County residents was down for approximately 6 hours August 25 before crews repaired technical issues caused by an overnight power outage.
Source: http://www.chicoer.com/general-news/20150825/1230-pm-update-9-1-1-system-restored-in-butte-county

Information Technology Sector

26. *August 26, SC Magazine* – (International) **Zero-day, Angler kit exploits help drive up malvertising by 325%.** Security researchers from Cyphort reported study findings revealing that malvertising attacks have increased by 325 percent in 2015, likely due to a combination of frequent zero-day exploits and new technology making the tactic more effective.
Source: http://www.scmagazine.com/spike-in-malvertising-attributed-to-zero-days-emergence-of-new-tech/article/434796/

27. *August 26, Securityweek* – (International) **New Zeus variant "Sphinx" offered for sales.** Malware developers released a new Zeus banking trojan variant called Sphinx that operates fully through The Onion Router (Tor) anonymity network and is designed to work on Microsoft Windows Vista and Windows 7 with User Account Control (UAC) enabled, as well as on low-privilege and "Guest" accounts. The malware has a full feature suite including Backconnect Virtual Network Computing (VNC) capability allowing users to transfer funds directly from the infected system.
Source: http://www.securityweek.com/new-zeus-variant-sphinx-offered-sale

28. *August 26, Threatpost* – (International) **CERT warns of hard-coded credentials in DSL SOHO routers.** The Computer Emergency Readiness Team (CERT) published an advisory warning that certain Digital Subscriber Line (DSL) routers manufactured by ASUS Tek, DIGICOM, Observa Telecom, Philippine Long Distance Telephone, and ZTE contain hard-coded credentials that could allow a hacker to remotely control or access the devices via telnet services.
Source: https://threatpost.com/cert-warns-of-hard-coded-credentials-in-dsl-soho-routers/114421

29. *August 26, Securityweek* – (International) **Sundown EK first to integrate exploit for recently patched IE flaw.** Security researchers from Symantec discovered that the Sundown exploit kit (EK) integrated a recently patched Microsoft Internet Explorer memory corruption vulnerability, and reported observing watering hole attacks leveraging the EK to deliver the Trojan.Nancrat backdoor.
Source: http://www.securityweek.com/sundown-ek-first-integrate-exploit-recently-patched-ie-flaw

30. *August 26, Threatpost* – (International) **Researchers uncover new Italian RAT uWarrior.** Security researchers from Palo Alto Networks discovered a new fully-featured remote access trojan (RAT) called uWarrior embedded in a rigged Rich Text Format (.RTF) file. After the file infects the system, it downloads a payload and is copied to another directory, where it communicates with a command and control server through an encrypted protocol.
Source: https://threatpost.com/researchers-uncover-new-italian-rat-uwarrior/114414

31. *August 26, V3.co.uk* – (International) **Apple iOS Ins0mnia flaw that hides malicious apps revealed by FireEye.** Security researchers from FireEye discovered that devices running versions of iOS prior to 8.4.1 are vulnerable to a flaw dubbed Ins0mnia, in which any application could bypass Apple background restrictions, and could allow an attacker to run in the background and steal sensitive user information indefinitely without the user's consent or knowledge.
Source: http://www.v3.co.uk/v3-uk/news/2423493/apple-ios-ins0mnia-flaw-that-hides-malicious-apps-revealed-by-fireeye

32. *August 25, IDG News Service* – (International) **Flaw in Android remote-support tool exploited by screen recording app.** Security researchers from Check Point discovered that the Recordable Activator Android app on Google Play was utilizing a recently discovered flaw in the TeamViewer remote support tool dubbed Certifi-gate, in which an attacker could use a rogue app to masquerade as an official tool and take control of an affected device. The app was pulled after having over 500,000 installations
Source: http://www.computerworld.com/article/2975776/security/flaw-in-android-remote-support-tool-exploited-by-screen-recording-app.html#tk.rss_security

33. *August 25, Threatpost* – (International) **AutoIt used in targeted attacks to move RATs.** Security researchers at Cisco discovered that hackers are using the AutoIt task automation freeware to stealthily drop remote access trojans (RATs) that install via malicious macros in Microsoft Word documents. AutoIt is considered a legitimate information technology (IT) administration tool, and is often whitelisted in enterprises.
Source: https://threatpost.com/autoit-used-in-targeted-attacks-to-move-rats/114406

For another story, see item **20**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

See items **31** and **32**

Commercial Facilities Sector

34. *August 26, WTKR 3 Norfolk* – (Virginia) **Roanoke reporter, photographer killed by shooter during live news interview.** A reporter and photographer from local news station WDBJ in Roanoke were killed by a shooter that appeared during a live news interview at Bridgewater Plaza in Moneta, Virginia, August 26. The shooter led police on a pursuit before being discovered in his vehicle with a self-inflicted gunshot wound. Source: http://wtkr.com/2015/08/26/suspected-active-shooter-investigation-involving-news-crew-underway-at-smith-mountain-lake/

35. *August 26, WPVI 6 Philadelphia* – (Pennsylvania) **Flames, ruptured gas line force 30 residents from Montco apartments.** A multi-alarm fire fueled by a ruptured gas line forced 30 residents from the Abrams Run Apartments in Upper Merion August 26. There are no reports of injuries and the cause of the fire remains under investigation. Source: http://6abc.com/news/flames-ruptured-gas-line-force-residents-from-montco-apts/957355/

36. *August 25, Richmond Times-Dispatch* – (Virginia) **Henrico fire displaces more than 25 at West End apartment complex.** More than 25 people were displaced from the Copper Spring Apartments in western Henrico County August 25 after 16 units were damaged by fire, smoke, or water. The cause of the fire remains under investigation. Source: http://www.richmond.com/news/local/henrico/article_4c6926da-f216-5bb0-8f8e-e69b404392ce.html

Dams Sector

37. *August 25, KSL Salt Lake City* – (Utah) **Salem canal breaks, community works to prevent flooding.** City workers and volunteers laid down sandbags in an effort to prevent water from flooding nearby homes after water was released from a breach in the Highline Canal in Salem, Utah, August 25. Gophers are being blamed for the breach, and officials turned off the canal for a couple days for inspection. Source: https://www.ksl.com/?sid=36156782&nid=148&title=salem-canal-breaks-community-works-to-prevent-flooding

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer